A GENERALIZATION OF FERMAT'S THEOREM.

By L. E. Dickson.

1. In a number of investigations, apparently not related to each other, there occurs the following function:

$$F(a,N) \equiv a^N - (a^{\frac{N}{p_1}} + a^{\frac{N}{p_2}} + \cdots + a^{\frac{N}{p_s}}) + (a^{\frac{N}{p_1p_2}} + a^{\frac{N}{p_1p_3}} + \cdots + a^{\frac{N}{p_{s-1}p_s}})$$

$$-(a^{\frac{N}{p_1p_2p_3}} + \cdots + a^{\frac{N}{p_{s-2}p_{s-1}p_s}}) + \cdots + (-1)^s a^{\frac{N}{p_1p_2\cdots p_s}},$$

a being any integer and N any positive integer whose distinct prime factors are $p_1, p_2, \ldots, p_s$. The theorem which we shall consider in the present paper is that $F(a,N)$ is divisible by N for every a and N. This theorem is a generalization of Fermat's theorem, to which it reduces when N is a prime.

In §§ 2–5 of the present paper it is explained how the function $F(a,N)$ has occurred in four distinct mathematical researches, and how from each of these points of view indirect proofs of the above mentioned generalized theorem have been obtained. In §6 two new direct proofs of this theorem are given. In §7 a third new direct proof is given, based upon a relation observed by Picquet. In §§7 and 8 some further properties of the function $F(a,N)$ are considered.

2. As far as known to the writer, the earliest occurrence of the function $F(a,N)$ is in an important paper by Schönemann.* He proved that, a being the power of a prime p^n, the number of congruences of degree N belonging to and irreducible in the Galois field of order $a = p^n$ is $\frac{1}{N} F(a,N)$. The same result was arrived at later by Pellet† and by the writer‡ independently. For $n = 1$, the result has been given by Serret§ and by Dedekind.‖ In none of these papers is there a reference to the earlier papers.

---

* Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist, *Crelle*, 31, 1846, pp. 269–325.

† *Comptes Rendus*, 70, 1870, pp. 328–330.

‡ *Bulletin of the American Mathematical Society*, July, 1897, pp. 381–389.

§ *Cours d'Algèbre supérieure*, 4th edition, Vol. 2, pp. 137–141.

‖ Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl-Modulus, *Crelle*, 54, 1857, pp. 1–26.

3. S. Kantor* has shown that the number of cyclic groups of order N in any Cremona transformation of order a in the plane is $\frac{1}{N}F(a,N)$. He first establishes the elegant recursion formula

$$(1) \qquad a^N - a = \sum_{d>1} F(a,d),$$

the sum extending over all the divisors $d > 1$ of N, including N itself. He derives from (1) the value of $F(a,N)$ by a lengthy method which he carries out for certain special cases. The result may, however, be derived immediately as follows. We give to (1) the following form, due to Dedekind for $a =$ prime:

$$(1') \qquad \iota^N = \sum_{d} F(a,d)$$

summed for every divisor d of N including N and unity. We have taken† $F(a,1) \equiv a$, in agreement with the fact that there are a distinct linear congruences modulo a, and p^n distinct linear congruences in the $GF[p^n]$. The determination of $F(a,N)$ as the general solution of (1') follows at once from the following important general theorem due to Dedekind (*l. c.* p. 21 and pp. 25–26):

If, for an arbitrary integer N, we have

$$F(N) = \sum_{d} f(d),$$

the sum extending over all the divisors of N, including N and unity, and if $p_1, p_2, \ldots, p_s$ are all the distinct prime factors of N, then

$$f(N) = F(N) - \sum_{i=1}^{s} F\left(\frac{N}{p_i}\right) + \sum_{i<j}^{1\ldots s} F\left(\frac{N}{p_i p_j}\right) - \sum_{i<j<k}^{1\ldots s} F\left(\frac{N}{p_i p_j p_k}\right) + \cdots$$

A similar theorem holds if $F(N) = \Pi f(d)$.

4. Picquet‡ was led to the number $F(a,N)$ in a wholly different connection. He considers the curves of order m having at a given point on a given cubic $3m-1$ consecutive points of intersection with the cubic. Such

---

* *Annali di Matematica* (Milano), (2) Vol. 10, pp. 64–73.

† See also end of §7.

‡ Picquet, Sur une généralisation du théorème de Fermat, *Comptes Rendus*, 96, 1883, p. 1136.

a C_m, although not completely determined, must meet the cubic in a further fixed point. Proceeding with the latter point as before, we obtain a particular kind of curvilinear polygon, only the vertices of which are determined. If the first point be suitably chosen, the polygon is a closed curve; it is at the same time inscribed and circumscribed to the given cubic. The number of the summits of the polygons of n sides is

$$F[(3m-1)^2, n] - 2F(1-3m,n)$$

which is therefore a multiple of n. There are $\frac{1}{n} F(3m-1,n)$ polygons with real summits situated on the branch of the cubic which contains its inflections, and a like number of polygons on the oval branch when the latter exists and when m is even.

5. Finally, G. Koenigs was led to the numerical function $F(a,N)$ in the theory of uniform substitutions.* Let $\phi(z)$ be a uniform function and denote by $\phi_n(z)$ the operation $\phi(z)$ repeated n times. Consider the equation

$$(E_n) \qquad z - \phi_n(z) = 0.$$

If n' divides n, every root of $E_{n'}$ is a root of E_n. Those roots of E_n which verify no like equation of lower index are said to belong to the index n. If x belong to the index n, so do also the quantities

$$x,\ \phi(x),\ \phi_2(x),\ \phi_3(x),\ \ldots,\ \phi_{n-1}(x),$$

which are permuted cyclically by the uniform substitution

$$z' = \phi(z).$$

The roots belonging to the index n are therefore distributed into circular groups of n roots each. If m be the degree of the polynomials forming the numerator and denominator of $\phi(z)$, the number of roots belonging to the exponent n is proved to be $F(m,n)$ by Koenigs. Hence this number is divisible by n.

6. We have therefore a number of indirect proofs of the divisibility of $F(a,N)$ by N, the quotient expressing certain enumerations. Picquet gave a direct proof, but required the consideration of various sub-cases. A more elementary proof was given by Ed. Lucas.†

---

* Sur une généralisation du théorème de Fermat, et ses rapports avec la théorie des substitutions uniformes, *Darboux Bull.* (2) VIII, p. 286.

† Lucas, Sur la généralisation du théorème de Fermat, *Comptes Rendus*, 96, 1883, p. 1300.

I have not had access to the proof given by Ed. Weyr.* I have recently found two very simple proofs of the theorem in question.

First proof. — Taking first the case in which N contains three distinct prime factors, $N \equiv r^\rho s^\sigma t^\tau$, we have

$$F(a,N) = (a^N - a^{\frac{N}{s}}) - (a^{\frac{N}{r}} - a^{\frac{N}{rs}}) - (a^{\frac{N}{t}} - a^{\frac{N}{ts}}) + (a^{\frac{N}{rt}} - a^{\frac{N}{rst}}).$$

Since each quantity in parenthesis is of the form

$$b^{s^\sigma} - b^{s^{\sigma-1}},$$

it is divisible by s^σ by Fermat's theorem. If N contained a fourth prime factor w, we should have in $F(a,N)$ four additional terms,

$$-(a^{\frac{N}{w}} - a^{\frac{N}{sw}}) + (a^{\frac{N}{rw}} - a^{\frac{N}{srw}}) + (a^{\frac{N}{tw}} - a^{\frac{N}{stw}}) - (a^{\frac{N}{rtw}} - a^{\frac{N}{srtw}}).$$

From the symmetry of $F(a,N)$, it follows that it is divisible by the other factors r^ρ, t^τ, etc.

Second proof. — The theorem follows immediately from the following congruence, which is readily verified:

$$[F(a, N)]^q - F(a, N) \equiv F(a, qN) \pmod q, \tag{2}$$

q being a prime number, while a and N are arbitrary integers. $F(a,qN)$ being therefore divisible by q, the theorem itself follows by simple induction.

We may put into evidence the divisibility of $F(a,N)$ by each of the prime factors of N simultaneously. For example,

$$F(a, rs) \equiv (a^r - a)^s - (a^r - a) \pmod s.$$

7. Theorem. — *The function $F(a,N)$ is characterized by the two properties,*

$$F(a, np^s) = F(a^{p^s}, n) - F(a^{p^{s-1}}, n) \tag{3}$$

$$F(a, p^s) = a^{p^s} - a^{p^{s-1}}, \tag{4}$$

where a is an arbitrary integer, n any integer not divisible by the prime number p.

We may verify by induction this theorem, stated without proof by Pic-

* Ueber einen Zahlen-theoretischen Satz, *Casopis, Zeitschrift zur Pflege der Mathematik und Physik*, XI, p. 39, 1882.

quet. Taking $n=q^r$, $q=$prime, we have as the first step in the induction, on applying (3) and (4),

$$F(a, q^r p^s) = (a^{p^s})^{q^r} - (a^{p^s})^{q^{r-1}} - (a^{p^{s-1}})^{q^r} + (a^{p^{s-1}})^{q^{r-1}},$$

giving therefore the function $F(a,N)$ of §1 for the case $N=q^r p^s$. To give the proof of the general step in the induction, we assume, for a given integer n having the prime factors $p_1, \ldots p_r$, and an arbitrary integer b, that the function $F(b, n)$ defined by (3) and (4) is precisely the function $F(b, n)$ of §1. Taking $b=a^{p^s}$ and $a^{p^{s-1}}$ in turn, we have by assumption the identities,

$$F(a^{p^s}, n) = a^{np^s} - (a^{\frac{n}{p_1}\cdot p^s} + \cdots + a^{\frac{n}{p_r}\cdot p^s}) + a^{\frac{n}{p_1 p_2}\cdot p^s} + \cdots\cdots$$

$$F(a^{p^{s-1}}, n) = a^{np^{s-1}} - (a^{\frac{n}{p_1}\cdot p^{s-1}} + \cdots + a^{\frac{n}{p_r}\cdot p^{s-1}}) + a^{\frac{n}{p_1 p_2}\cdot p^{s-1}} + \cdots\cdots$$

Hence if p be a prime number not contained in n, we have by applying (3),

$$F(a, np^s) = a^{np^s} - (a^{np^{s-1}} + a^{\frac{np^s}{p_1}} + \cdots + a^{\frac{np^s}{p_r}}) + (a^{\frac{np^s}{p\,p_1}} + \cdots + a^{\frac{np^s}{p\,p_r}} + a^{\frac{np^s}{p_1 p_2}} + \cdots) - \cdots\cdots,$$

which is precisely the function $F(aN)$ of §1, for $N=np^s$.

As a corollary we may derive a very simple proof (not observed by Picquet however) of the divisibility of $F(a,N)$ by N. The function $F(a, p^s)$ defined by (4) is divisible by p^s by Fermat's theorem. If then we assume that $F(a,n)$ is divisible by n for a arbitrary, it follows from (3) that $F(a, np^s)$ is divisible by n, p being a prime not contained in n. Our corollary thus follows by induction. This proof is closely related to the first proof given in §6.

We may generalize the relation (3) as follows. If m have the distinct prime factors $r, s, t, \ldots, w$ and if n be relatively prime to m, then

$$F(a,nm) = F(a^m,n) - F(a^{\frac{m}{r}},n) - F(a^{\frac{m}{s}},n) - \cdots\cdots - F(a^{\frac{m}{w}},n) + F(a^{\frac{m}{rs}},n) + \cdots\cdots + F(a^{\frac{m}{vw}},n) - \cdots\cdots \pm F(a^{\frac{m}{rs\cdots w}},n).$$

This formula reduces to that of §1 for $n=1$, $m=N$, provided we take $F(b, 1) \equiv b$.

8. An interesting number-theoretic property of the function $F(a,N)$ is given by the following theorem, which I believe to be new:

If $\phi(d)$ *denotes the number of positive integers prime to* d *and not exceeding* d, *then, for arbitrary integers* a *and* N *greater than unity,*

$$\sum_d \phi(d) = F(a,N)$$

the sum extending over all proper divisors of $a^N - 1$.

By a *proper* divisor of a^N-1 we understand one which does not divide a^m-1 if $m < N$. Thus, the proper divisors of $6^4 - 1$ are $3\cdot7\cdot37$, $5\cdot37$, $7\cdot37$, and 37; the sum of their ϕ's equals $35\cdot36 = 6^4 - 6^2 = F(6,4)$. Again, the proper divisors of 6^6-1 are $5\cdot7\cdot31\cdot43$, $5\cdot31\cdot43$, $7\cdot31\cdot43$, $5\cdot7\cdot43$, $31\cdot43$, $7\cdot43$, $5\cdot7\cdot31$, $7\cdot31$, $5\cdot31$, and 31, the sum of whose ϕ's equals $30\cdot1547 = 6^6 - 6^3 - 6 + 6 = F(6,6)$.

The proof of the theorem follows immediately from the above general theorem of Dedekind, if we note that

$$\sum_n \sum_d \phi(d) = a^N - 1,$$

n running through all the divisors of N including N and unity. Further, $F(a,N)$ is unchanged if we replace every term $a^{\frac{N}{K}}$ by $a^{\frac{N}{K}} - 1$, the added terms being given by the expansion of $-(1-1)^s$.

UNIVERSITY OF CALIFORNIA, APRIL, 1899.